Resko, dnia 21.10.2021 r.

...............................................................

pieczęć zamawiającego

ZAPYTANIE OFERTOWE Nr ZP.271.16.21.ZPOF

Mając na uwadze zamiar udzielenia zamówienia nie podlegającego ustawie z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 ze zm.), zgodnie z art.2 ust 1 pkt 1 przytaczanej wyżej ustawy, zapraszamy do złożenia ofert na usługę pn.: „Prowadzenie audytu w zakresie zgodności z przepisami RODO na poziomie prawnym i informatycznym w Urzędzie Miejskim w Resku”.

Oferty mogą być złożone przez usługodawców spełniających warunki określone w art.279 i 286 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2021 r., poz. 305 ze zm.), zwaną dalej ustawą.

1. **Zamawiający:** Gmina Resko reprezentowana przez Burmistrza Reska, p. Arkadiusza Czerwińskiego, ul. Rynek 1, 72-315 Resko, tel. 91 39 51 503, fax. 91 39 51 205 e-mail: [zamowienia@resko.pl](mailto:zamowienia@resko.pl)
2. **Opis przedmiotu zamówienia:**
3. **Przedmiotem zamówienia jest usługa pn.: *„Prowadzenie audytu w zakresie zgodności z przepisami RODO na poziomie prawnym i informatycznym w Urzędzie Miejskim w Resku”.***
4. **Termin realizacji:**  **30 dni od dnia podpisania umowy.**
5. Przedmiot zamówienia obejmuje przeprowadzenie kompleksowego audytu wewnętrznego z zakresu stosowania przepisów Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dn. 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych w Urzędzie Miejskim w Resku.

Zakres audytu:

* środki techniczne
* środki organizacyjne
* dokumentacja ochrony danych
* sposób realizowania obowiązków przez osoby upoważnione

Audyt obejmować będzie następujące czynności:

a) weryfikację i ocenę organizacji systemu ochrony danych osobowych w Urzędzie,

b) weryfikację i ocenę prawa do przetwarzania danych osobowych,

c) weryfikację sposobu realizacji praw osoby, której dane dotyczą oraz jego ocenę,

d) weryfikację i ocenę sposobu rejestrowania czynności przetwarzania danych osobowych,

e) weryfikację i ocenę sposobu przeprowadzenia oceny skutków przetwarzania danych osobowych,

f) weryfikację i ocenę procedur związanych z identyfikacją i zgłoszeniem naruszenia przetwarzania danych osobowych,

g) wydanie rekomendacji w odniesieniu do obszarów wskazanych w pkt a - f, wskazujących na prawidłowe rozwiązania, w przypadku negatywnych praktyk – wskazanie sposób ich rozwiązania,

h) sporządzenie raportu kontroli zawierającego rekomendacje rozwiązań ewentualnych niezgodności.

Przeprowadzenie zadania audytowego będzie odbywało się w budynku Urzędu Miejskiego w Resku. Techniki wykorzystane do przeprowadzenia audytu:

1. Badanie udostępnionych dokumentów i plików.

2. Uzyskanie wyjaśnień od kierownictwa i pracowników administratora danych.

3. Dokonanie oględzin obszarów przetwarzania danych osobowych w budynku Urzędu oraz na wybranych w uzgodnieniu z IOD 4 stanowiskach pracy.

1. **Zakres usługi w przedmiocie audytu bezpieczeństwa informacji we wszystkich obszarach funkcjonowania organizacji:**
2. Audyt organizacyjny:
3. Regulacje w obszarze zarządzania bezpieczeństwem informacji;
4. Odpowiedzialność za bezpieczeństwo informacji i koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji;
5. Dokumentacja z zakresu ochrony danych osobowych;
6. Przeprowadzenie wywiadów z wybranymi pracownikami.
7. Audyt fizyczny i środowiskowy:
8. Weryfikacja granic obszaru bezpiecznego;
9. Weryfikacja zabezpieczeń wejścia/wyjścia;
10. Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń;
11. Weryfikacja bezpieczeństwa okablowania strukturalnego;
12. Weryfikacja systemów chłodzenia;
13. Weryfikacja systemów alarmowych.
14. Audyt teleinformatyczny:
15. Weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi;
16. Weryfikacja ochrony przed oprogramowaniem szkodliwym;
17. Weryfikacja procedur zarządzania kopiami zapasowymi;
18. Weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
19. Weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe;
20. Weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania);
21. Analiza i ocena mechanizmów zarządzania aktualizacjami.
22. Audyt ochrony danych osobowych:
23. Przegląd zgodności przetwarzania danych osobowych z wymaganiami Ustawy;
24. Przegląd istniejących regulacji wewnętrznych odnośnie bezpieczeństwa przetwarzania danych osobowych;
25. Przegląd aktualnie wykorzystywanych dokumentów mających związek z ochroną danych osobowych;
26. Identyfikacja zbiorów potencjalnie podlegających rejestracji.
27. Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej:
28. Testy styku sieci lokalnej z internetem przeprowadzane ze stacji roboczej podłączonej do sieci internet;
29. Analiza topologii brzegu sieci;
30. Weryfikacja mechanizmów ochronnych;
31. Próba wykrycia usług sieciowych udostępnianych do internetu;
32. Detekcja wersji oraz typu oprogramowania dostępnego z sieci internet;
33. Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci internet;
34. Przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią internet.
35. Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji:
36. Analiza topologi sieci LAN;
37. Weryfikacja mechanizmów ochronnych w sieci;
38. Analiza komunikacji sieciowej;
39. Skanowanie portów TCP/UDP próba wykrycia usług sieciowych;
40. Skanowanie hostów aktywnych w sieci;
41. Exploitacja dostępnych urządzeń oraz usług w sieci LAN;
42. Przedstawienie rozwiązań zwiększających bezpieczeństwo w sieci LAN.
43. Badanie odporności użytkowników na socjotechniki.

Zakres testów socjotechnicznych:

1. Telefoniczny kontakt z użytkownikiem w celu próby pozyskania informacji niejawnych;
2. Kontakt mailowy z próbami pozyskania danych logowania (phishing);
3. Kontakt mailowy z próbami aktywowania wirusów / trojanów;
4. Kontakt bezpośredni w celu uzyskania nieautoryzowanego dostępu do zasobów firmy;
5. Próby podszycia się pod osobę znaną w celu nakłonienia do określonych działań zagrażających bezpieczeństwu.
6. Wskazanie obszarów niezgodności z RODO i zaproponowanie działań dostosowujących
7. Wykonanie i przekazanie Raportów z Audytu z omówieniem.
8. Raport z zaleceniami należy sporządzić w wersji papierowej (2 egzemplarze) i na nośniku CD/DVD.
9. Istotne informacje dotyczące realizacji audytu:
   1. liczba pracowników: 29
   2. liczba lokalizacji: 1,
   3. liczba serwerów: fizycznych (4)
   4. liczba stacji roboczych: 29,
   5. liczba urządzeń sieciowych: 10,
   6. liczba IP adresów zew., które mają być objęte testami zew.: 5,
   7. liczba baz danych, które mają być objęte audytem: 5,
   8. dokumentacja w zakresie ochrony danych osobowych: Polityka bezpieczeństwa danych osobowych, Polityka bezpieczeństwa informacji, Instrukcja zarządzania systemami informatycznymi, rejestr upoważnień do przetwarzania danych osobowych, ewidencja zgód na przebywanie w obszarze przetwarzania danych osobowych, jawny rejestr zbiorów danych osobowych, rejestr sprzętu i oprogramowania, rejestr podmiotów przetwarzających dane osobowe na podstawie umowy powierzenia, rejestr druków nadania / zmiany / usunięcia uprawnień, rejestr incydentów, ewidencja udostępniania danych osobowych.
10. **Istotne postanowienia do umowy:**
    1. zawarcie umowy zlecenie z wybranym wykonawcą,
    2. umowa zlecenie zawarta przez Urząd Miejski w Resku zawierać będzie postanowienia gwarantujące prowadzenie audytu zgodnie z przepisami prawa.
    3. w umowie zlecenia zostanie określony sposób postępowania z dokumentami, wytwarzanymi dla celów prowadzenia audytu, tak aby zapewnić ich dostępność, ochronę przed nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem.
11. **Usługodawcą, o którym mowa w art. 275 pkt 2 ustawy może być:**
    1. osoba fizyczna, spełniająca warunki określone w art. 286 ustawy;
    2. osoba fizyczna prowadząca działalność gospodarczą, spełniająca warunki określone w art. 286 ustawy;
    3. spółka cywilna, spółka jawna, spółka partnerska, spółka komandytowa, spółka komandytowo-akcyjna lub osoba prawna, która zatrudnia do prowadzenia audytu wewnętrznego w jednostce osoby spełniające warunki określone w art. 286 ustawy.
12. **Wykonawca musi spełniać niżej wymienione wymagania:**
13. ma obywatelstwo państwa członkowskiego Unii Europejskiej lub innego państwa, którego obywatelom, na podstawie [umów](https://sip.lex.pl/#/hipertekst/17569559_art%28286%29_1?pit=2017-05-10) międzynarodowych lub przepisów prawa wspólnotowego, przysługuje prawo podjęcia zatrudnienia na terytorium Rzeczypospolitej Polskiej;
14. ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych*;*
15. nie była karana za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
16. posiada wyższe wykształcenie;

**Wykonawca musi wykazać, że w okresie ostatnich 3 lat wykonał lub wykonuje należycie co najmniej trzy usługi, polegające na prowadzeniu kompleksowego audytu z zakresu stosowania przepisów Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dn. 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych dla jednostki administracji publicznej.**

**Na potwierdzenie prawidłowej realizacji usługi wykonawca załączy dokumenty poświadczające (referencje), wystawione przez jednostkę na rzecz której usługa była lub jest świadczona.**

**Wykonawca musi dysponować co najmniej jedną osobą, która będzie realizowała przedmiot niniejszego zamówienia i posiadała doświadczenie polegające na wykonaniu lub wykonywaniu w ciągu ostatnich 3 lat co najmniej trzech usług, polegających na prowadzeniu kompleksowego audytu z zakresu stosowania przepisów Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dn. 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych dla jednostki administracji publicznej.**

Zamawiający wykluczy z postępowania wykonawców, którzy w przeszłości wykonywali audyty na rzecz Gminy Resko.

1. **Kryterium oceny ofert:** cena 100%

Cena musi być podana w złotych polskich, w kwocie brutto (z uwzględnieniem podatku VAT).

Cena obejmuje wszystkie koszty Wykonawcy.

**Zamawiający udzieli zamówienia Wykonawcy, który zaoferuje najniższą cenę za wykonanie przedmiotu zamówienia.**

1. **Sposób przygotowania oferty:**

**Ofertę sporządzić należy na załączonym druku „Formularz ofertowy Wykonawcy” (załącznik 1).** Ofertę sporządzić należy w języku polskim, w formie pisemnej, na maszynie, komputerze, lub inną trwałą techniką. Oferta winna być podpisana przez osobę upoważnioną.

**Na ofertę składają się następujące dokumenty:**

1. formularz ofertowy wykonawcy – załącznik nr 1
2. oświadczenie wykonawcy o spełnieniu warunków, o których mowa w art. 286, ust. 1, pkt 1-3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2021 r., poz. 305 ze zm., - w treści formularza ofertowego
3. wykaz usług wykonanych lub wykonywanych w ciągu ostatnich 3 lat wraz z dokumentami poświadczającymi ich prawidłowe wykonywanie – załącznik nr 2
4. personel wykonawcy - wykaz osób, które będą bezpośrednio realizować przedmiot zamówienia, ze wskazaniem ich wykształcenia, kwalifikacji i doświadczenia zawodowego oraz funkcji, jaką będą pełnić podczas realizacji zamówienia – załącznik nr 3; do wykazu należy załączyć potwierdzone za zgodność z oryginałem kopie dokumentów potwierdzających wykształcenie oraz kwalifikacje do przeprowadzenia audytu zgodnie z wymaganiami Zamawiającego.

Ofertę należy sporządzić na druku stanowiącym załącznik n1 – „OFERTA”, wypełnić odręcznie lub komputerowo. Oferta winna być podpisana odręcznie lub elektronicznie podpisem zaufanym, osobistym lub kwalifikowanym podpisem elektronicznym przez osobę upoważnioną. Ofertę należy złożyć poprzez platformę zakupową pod adresem: <https://platformazakupowa.pl/transakcja/524743>

1. **Termin złożenia oferty:** ofertę złożyć należy **do dnia 03.11.2021 r., do godz. 10:00.**

Burmistrz Reska

Arkadiusz Czerwiński

**Załącznik nr 1   
do zapytania ofertowego   
nr ZP.271.16.21.ZPOF**

**FORMULARZ OFERTOWY WYKONAWCY**

na wykonanie zamówienia publicznego pod nazwą :

***„*Prowadzenie audytu w zakresie zgodności z przepisami RODO   
na poziomie prawnym i informatycznym w Urzędzie Miejskim w Resku*”***

**1. Dane dotyczące Wykonawcy:**

Nazwa / imię i nazwisko……………………………………………………………………

Siedziba / adres…………………………………………………………………………….

Nr telefonu/faks …………………………………………………………………………….

adres e-mail: ………………………………………………………………………………..

nr NIP………………………………….……………………………………………………..

nr REGON ……………………………….………………………………………………….

nr PESEL ……………………………………………………………………………………

# Dane dotyczące Zamawiającego :

**Gmina Resko reprezentowana przez**

**p. Arkadiusza Czerwińskiego – Burmistrza Reska**

ul. Rynek 1, 72 – 315 Resko

1. **Zobowiązania Wykonawcy:  
   Zobowiązuję się wykonać przedmiot zamówienia za cenę ryczałtową :**

**Cena wykonania zamówienia brutto : …………………………. zł**

(słownie: ………………………………………………………..............…………………)  
  
 **Kwota netto = …………………………. zł, Wartość podatku = …………………….. zł**

**Stawka podatku ….. %**

1. **Oświadczenia Wykonawcy:** 
   * 1. Uważam się za związanego ofertą przez okres 30 dni od dnia składania ofert.
     2. Dysponuję wiedzą, doświadczeniem, potencjałem technicznym, ekonomicznym  
        i finansowym niezbędnym do prawidłowego zrealizowania przedmiotu zamówienia.
     3. Dysponuję lub będę dysponował osobami zdolnymi do prawidłowego wykonania przedmiotu zamówienia
     4. Mam obywatelstwo państwa członkowskiego Unii Europejskiej lub innego państwa, którego obywatelom, na podstawie umów międzynarodowych lub przepisów prawa wspólnotowego, przysługuje prawo podjęcia zatrudnienia na terytorium Rzeczypospolitej Polskiej;
     5. Mam pełną zdolność do czynności prawnych oraz korzystam z pełni praw publicznych;
     6. Nie byłem karany za umyślne przestępstwo lub umyślne przestępstwo skarbowe;

…………………………………… ………………………………………….

*Pieczęć Wykonawcy data, imię i nazwisko, podpis osoby uprawnionej*

**Załącznik nr 2   
do zapytania ofertowego   
nr ZP.271.16.21.ZPOF**

**Zamawiający:**Gmina Resko   
ul. Rynek 1, 72-315 Resko

**Wykonawca:**

………………………………………………………………………………………..

…………………………………………..

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

…………………………………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

## Wykaz usług wykonanych w okresie ostatnich 3 lat

dotyczy zamówienia publicznego pn.

**„*Prowadzenie audytu w zakresie zgodności z przepisami RODO   
na poziomie prawnym i informatycznym w Urzędzie Miejskim w Resku*”**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LP | Określenie usługi z krótkim opisem  i podaniem podstawowych parametrów | Wartość  Usługi | Termin realizacji | Nazwa Zamawiającego |
| **1.** |  |  |  |  |
| **2.** |  |  |  |  |
| **3.** |  |  |  |  |

Do niniejszego wykazu załączam dowody potwierdzające, że usługi zostały wykonane należycie lub są realizowane należycie (referencje).

|  |  |
| --- | --- |
| …………………………………………………  Miejscowość, data | .............................................................................  Podpis upoważnionych przedstawicieli Wykonawcy |

**Załącznik nr 3   
do zapytania ofertowego   
nr ZP.271.16.21.ZPOF**

**Zamawiający:**Gmina Resko   
ul. Rynek 1, 72-315 Resko

**Wykonawca:**

………………………………………………………………………………………..

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

…………………………………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**PERSONEL WYKONAWCY**

dotyczy zamówienia publicznego pn.

**„*Prowadzenie audytu w zakresie zgodności z przepisami RODO   
na poziomie prawnym i informatycznym w Urzędzie Miejskim w Resku*”**

Dane osób, które będą uczestniczyć w realizacji zadania :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Imię i nazwisko**  **Podstawa dysponowania osobą np. umowa o pracę, umowa zlecenie, pisemne zobowiązanie** | **Przewidywana rola w realizacji zamówienia** | **Posiadane wykształcenie, kwalifikacje** | **Informacje nt. wiedzy i doświadczenia w zakresie zgodnym z wymaganiami Zamawiającego określonymi w zapytaniu ofertowym** |
|  |  |  |  |  |
|  |  |  |  |  |

**Oświadczam, że osoby, które będą uczestniczyć w wykonywaniu zamówienia, wskazane powyżej, spełniają wymagania określone w treści zapytania ofertowego, tj.: co najmniej jedna osoba posiada doświadczenie polegające na wykonaniu lub wykonywaniu w ciągu ostatnich 3 lat co najmniej trzech usług, polegających na prowadzeniu kompleksowego audytu wewnętrznego z zakresu stosowania przepisów Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dn. 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych dla jednostki administracji publicznej.**

**Załączam dokumenty potwierdzające posiadanie przez wyżej wymienione osoby wskazanego wykształcenia, kwalifikacji oraz doświadczenia.**

|  |  |  |  |
| --- | --- | --- | --- |
| …………………………………………………  Miejscowość, data | .............................................................................  Podpis upoważnionych przedstawicieli Wykonawcy |  |  |